ROSEMBERG FARIA CALHEIROS

SEGURANÇA DE INFORMAÇÕES NAS EMPRESAS

uma prioridade corporativa

Rio de Janeiro
2002

ROSEMBERG FARIA CALHEIROS

SEGURANÇA DE INFORMAÇÕES NAS EMPRESAS
uma prioridade corporativa

Trabalho de Conclusão de Curso apresentado à Escola de Biblioteconomia da Universidade do Rio de Janeiro, como requisito parcial para obtenção do grau de Bacharel em Biblioteconomia

Orientador: Profª. ESP. Iris Abdallah Cerqueira

Rio de Janeiro
2002

ROSEMBERG FARIA CALHEIROS

SEGURANÇA DE INFORMAÇÕES NAS EMPRESAS
uma prioridade corporativa

Trabalho de Conclusão de Curso apresentado à Escola de Biblioteconomia da Universidade do Rio de Janeiro, como requisito parcial para obtenção do grau de Bacharel em Biblioteconomia

Aprovado em de 2002.

BANCA EXAMINADORA

____
Prof. MS. Eugênio Decourt
Universidade do Rio de Janeiro

____
Profª. Maria Tereza Reis Mendes
Universidade do Rio de Janeiro

____
Profª. ESP. Iris Abdallah Cerqueira
Universidade do Rio de Janeiro

AGRADECIMENTOS

À Deus, em primeiro lugar, que me deu sabedoria;

À minha esposa Antônia Aguiar Calheiros, que sempre me incentivou em todos os momentos;

À professora Íris Abdallah Cerqueira minha orientadora, pelo incentivo, apoio e total atenção ao longo do curso, para que este trabalho fosse concretizado;

Aos meus amigos e professores da UNIRIO, pelo convívio, aprendizado e marcante amizade.

LISTA DE ILUSTRAÇÕES

Figura 1 - Agentes envolvidos em uma relação agente-ativo..................................17

Figura 2 - Ciclo da Segurança da Informação...20

Figura 3 - Ameaças da segurança...26

Gráfico 1 - Principais ameaças às informações da empresa...................................28

Fluxograma 1 - Modelo de esquema organizacional para grupos de contingência..35

RESUMO

Objetiva a conscientização da importância da segurança das informações nas empresas e instituições, na elaboração de um planejamento de segurança eficaz para, assim, protegê-las de maiores riscos, uma vez que a informação é um bem de valor intangível. Apresenta recursos e medidas relacionadas à proteção da informação e os riscos relativos às vulnerabilidades. Ressalta a importância de estratégias na identificação das necessidades adequadas à segurança da informação. Cita as causas de ameaças à segurança na integridade das informações e meios de prevenção. Aborda os controles adotados na prevenção de incidentes, definindo soluções para minimizar os riscos de segurança. Revela os elementos necessários nos processos confidenciais, mediante atuação efetiva de todos as pessoas, evitando, assim, falhas que possam afetar o bom funcionamento da empresa ou instituição.

Palavras-chave: Segurança de informações. Planejamento de segurança. Vulnerabilidade.

ABSTRACT

Objective to acquire knowledge about the importance of the security of the information in the companies and institutions, in the elaboration of a planning of efficient security for, thus, protecting it of bigger risks, a time when the information is a good of intangible value. It presents resources and measures related to the relative protection of the information and risks to the vulnerabilities. The importance of strategies in the identification of the adequate needs to the security of the information standes out. It cites the causes of threats to the security in the integrity of the information and ways of prevention. It approaches the controls adopted in the prevention of incidents, defining solutions to minimize the security risks. It discloses the necessary elements in the confidential processes, in an performance that accomplishes all the people, thers preventing, imperfections that can affect the good functioning of the company or institution.

Keywords: Security of information. Planning of security. Vulnerability.

SUMÁRIO

1 **INTRODUÇÃO**........ 11
2 **CONCEITOS**........ 12
3 **OBJETIVOS DA SEGURANÇA**........ 13
4 **ANÁLISE DE RISCO**........ 16
4.1 *Ativos*........ 17
4.2 *Risco*........ 17
5 **VULNERABILIDADE**........ 19
5.1 *Tipos de vulnerabilidades*........ 19
6 **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**........ 21
6.1 *Objetivos*........ 21
6.2 *Controles necessários*........ 21
6.3 *Classificação de informações*........ 21
7 **CONTROLE DE ACESSO FÍSICO**........ 24
7.1 *Segurança física*........ 24
7.2 *Recursos a serem protegidos*........ 24
8 **CONTROLE DE ACESSO LÓGICO**........ 24
8.1 *Segurança lógica*........ 24
8.2 *Senha*........ 24
9 **PRINCIPAIS AMEAÇAS DE SEGURANÇA**........ 26
9.1 *Integridade*........ 26
9.2 *Indisponibilidade*........ 26
9.3 *Divulgação da informação*........ 26
9.4 *Alterações não autorizadas*........ 26
10 **ORIGENS DAS AMEAÇAS**........ 27
10.1 *Ameaças internas*........ 27

10.2 *Fraudes cometidas por funcionários*.. 27
10.3 *Roubo de informações*... 28
10.4 *Erros humanos*.. 29
10.5 *E-mail*.. 29
10.6 *Vírus*... 29
10.7 *Treinamento inadequado*... 30
10.8 *Pirataria*.. 30
10.9 *Ameaças externas*.. 32
10.9.1 Invasores.. 32
11 **PLANO DE CONTINGÊNCIA**.. 35
12 **AUDITORIA**... 36
12.1 *Auditoria interna*... 36
13 **CONCLUSÃO**.. 37
REFERÊNCIAS... 38
GLOSSÁRIO... 41
ANEXO A.. 44

1 INTRODUÇÃO

Na era do conhecimento, onde a informação é considerada um dos principais patrimônios de grande parte das organizações, ela deve ser tratada como tal, devendo ser protegida nos seus aspectos de disponibilidade, integridade e confidencialidade. Isto porque a segurança de informações é um elemento chave dentro desse conceito.

A segurança de informações não deve ser vista como "guardar num cofre todas as informações disponíveis", mas elaborar políticas de proteção das informações a fim de se evitarem maiores riscos e vulnerabilidades.

A segurança de informação tem deixado de ser tratada como um assunto técnico da área de informática, e vem sendo considerada uma real necessidade nas empresas e nas instituições, visto que a informação é o bem ativo mais valioso de uma empresa. A segurança passa a ser um requisito estratégico, que interfere na capacidade das organizações de realizarem negócios e no valor de seus produtos no mercado.

Uma boa Política de Segurança da Informação deve ser composta por regras claras, praticáveis e sintonizadas com a cultura e o ambiente tecnológico da empresa. Deve não apenas proteger não só as informações confidenciais, mas também motivar as pessoas que as manuseiam, mediante a conscientização e envolvimento de todos. Garantir a segurança coorporativa é um grande desafio, que passa por todas as pessoas envolvidas, direta e indiretamente.

Segurança é, portanto, a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não-autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança.

2 CONCEITOS

Segundo alguns conceitos básicos de escritores para fundamentação do trabalho, a Segurança de informação é o conjunto de dados, imagens, textos e outras formas de representação usadas para os valores da Companhia, associados ao seu funcionamento e/ou manutenção das suas vantagens competitivas.

Conforme a Política de Segurança da Informação em POLÍTICAS, (2002), os conceitos podem ser definidos como:

Recursos de Informação - são todos os meios usados para obtenção, geração, armazenamento e transporte das informações. Inclui: os recursos do ambiente de tecnologia da informação (instalações e equipamentos de informática e telecomunicações, sistemas operacionais, aplicativos e sistemas de informação usados nesses equipamentos) e outros recursos convencionais (arquivos, papel, microfilme, mapas etc...).

Sistema de Informação - é um conjunto de processos e recursos do ambiente de tecnologia da informação organizados para prover, de modo sistemático, informações para a Companhia.

Órgão Proprietário da Informação - é o órgão da empresa responsável pelas informações de uma determinada área de atividade da Companhia.

Proprietário da Informação - empregado, designado pelo Órgão Proprietário da Informação, para responder perante a Companhia pela classificação das informações e definição das suas necessidades de segurança.

Comitê de Segurança de Informações - é o comitê constituído pela Diretoria Executiva da empresa com a finalidade de implantar e garantir o cumprimento da Política de Segurança de Informações no âmbito da Companhia.

Gerente de Segurança de Informações do Órgão - empregado designado pelo órgão da Companhia, como responsável pelo cumprimento da Política de Segurança de Informações no âmbito do órgão, servindo de interface entre gerentes, proprietários, usuários, custodiantes, Gerência de Tecnologia da Informação do Órgão e o Comitê de Segurança de Informações.

3 OBJETIVOS DA SEGURANÇA

Quando se pensa em segurança de informações, a primeira idéia que nos vem à mente é a proteção da mesma, não importando onde ela esteja. Um sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como esperado. Porém, segurança é um conceito que vai muito além disso. É expectativa de todos que a informação armazenada em um sistema computacional permaneça lá, sem que pessoas não autorizadas tenham acesso a seu conteúdo. Ou seja, é expectativa de qualquer usuário que as informações estejam em local adequado, disponíveis no momento desejado, que sejam confiáveis, corretas e permaneçam protegidas contra acessos indesejados. Essas expectativas correspondem aos objetivos da segurança.

Destacam-se entre os objetivos da segurança (SEGURANÇA da tecnologia, 2001):

Confidencialidade ou privacidade – proteger as informações contra acesso de qualquer pessoa não autorizada pelo gestor da informação. Este objetivo envolve medidas como controle de acesso e criptografia.

Integridade dos dados – evitar que dados sejam apagados, ou alterados sem a permissão do gestor da informação.

Legalidade - Estado legal da informação, em conformidade com os preceitos da legislação em vigor.

Disponibilidade – garantir o provimento do serviço de informática, sob demanda, sempre que necessário aos usuários autorizados. As medidas relacionadas a esse objetivo podem ser duplicação de equipamentos/sistemas e *backup*. Um bom exemplo de ataque contra disponibilidade é a sobrecarga provocada por usuários ao enviar enormes quantidades de solicitação de conexão com o intuito de provocar pane nos sistemas.

Consistência – certificar-se de que o sistema atua de acordo com a expectativa dos usuários.

Isolamento ou uso legítimo – controlar o acesso ao sistema. Garantir que somente usuários autorizados possuam acesso ao sistema.

Auditoria – proteger os sistemas contra erros e atos cometidos por usuários autorizados. Para identificar autores e ações, são utilizadas trilhas de auditorias e *logs*, que registram o que foi executado no sistema, por quem e quando.

Confiabilidade – garantir que, mesmo em condições adversas, o sistema atuará conforme esperado.

Antes de implementar um programa de segurança de informações, é aconselhável responder às seguintes questões:

a) o que proteger?
b) contra que ou quem?
c) quais as ameaças mais prováveis?
d) qual a importância de cada recurso?
e) qual o grau de proteção desejado?
f) quanto tempo, recursos humanos e financeiros se pretende gastar para atingir os objetivos de segurança desejados?
g) quais as expectativas dos usuários e clientes em relação à segurança de informações?
h) quais as conseqüências para a instituição se seus sistemas e informações forem violados ou roubados?

Tendo a resposta a essas perguntas, é definida a política de segurança de informações e analisadas as ameaças, fazendo-se uma análise de riscos. A tecnologia de segurança a ser implantada deve atender aos requisitos da política. Por fim, para administrar os sistemas, é necessário implantar uma gerência de segurança.

Segurança de Informação é a conjugação de uma estratégia e de ferramentas específicas que atendam as necessidades corporativas para a manutenção de um ambiente saudável. Considerada um item vivo, a política de segurança nunca está

acabada e deve ser desenvolvida e atualizada durante toda a vida da empresa. (COLTRO, 2002, p. 26).

4 ANÁLISE DE RISCO

Conforme Moreira (2001, p. 11):

> a análise de risco consiste em um processo de identificação e avaliação dos fatores de risco presentes e de forma antecipada no Ambiente Organizacional, possibilitando uma visão do impacto negativo causado aos negócios. Através da aplicação desse processo, é possível determinar as prioridades de ação em função do risco identificado, para que seja atingido o nível de segurança desejado pela Organização. Proporciona também informações para que se possa identificar, antecipadamente, o tamanho e o tipo de investimento necessário para prevenir os impactos na Organização causados pela perda ou indisponibilidade dos recursos fundamentais para o negócio.

As medidas de segurança não podem assegurar 100% de proteção, e a empresa deve analisar a relação custo/benefício de todas. A empresa precisa achar o nível de risco que estará disposta a correr (MOREIRA, 2001, p. 12)

Segundo Moreira (2001, p. 12), o processo da análise de risco deve, no mínimo, proporcionar as seguintes informações:

a) pontos vulneráveis do ambiente;
b) ameaças potenciais ao ambiente;
c) incidentes de segurança causado pela ação de cada ameaça;
d) impacto negativo para o negócio a partir de cada incidente de segurança;
e) medidas de proteção adequadas para impedir ou diminuir o impacto de cada incidente.

Podemos considerar que a Análise de Risco é peça fundamental para obtenção da qualidade de um Programa de Segurança, pois ajudará a identificar todos os pontos críticos e falhos de proteção em todos os processos, configurações, documentos, enfim, tudo que possa ser valioso para a atividade da Organização.

Essa atividade fornecerá diretrizes para a identificação das medidas de segurança necessárias para que o ambiente computacional da empresa possa atingir o nível de segurança desejado.

Citam-se entre os aspectos a considerar na análise de risco:

4.1 *Ativos*

Ativos são os elementos que manipulam direta ou indiretamente, uma informação, inclusive a própria informação dentro de uma Organização, e é isso que devem ser protegidos contra ameaças para que o negócio funcione corretamente. Uma alteração, destruição, erro ou indisponibilidade de algum dos ativos podem comprometer os sistemas e, em decorrência, o bom funcionamento das atividades de uma empresa. Portanto, um dos passos da Análise de Risco é o de identificar todas as coisas que podem ser afetadas por um problema de segurança e que, neste caso, precisam ser protegidas (MOREIRA, 2001, p. 20)

PROPRIETARIO
CUSTODIANTE
ATIVO
USUÁRIO
CONTROLADOR

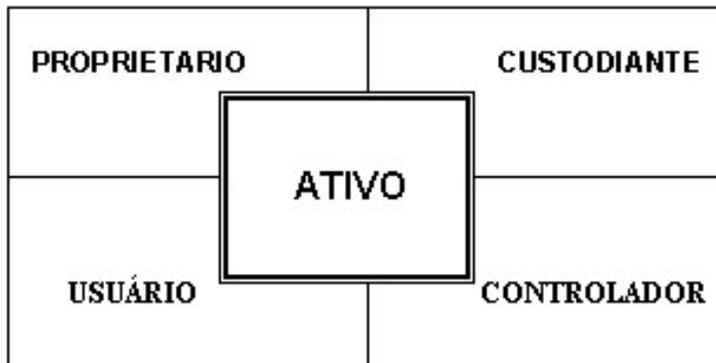



Figura 1 - Agentes envolvidos em uma relação agente-ativo.
Fonte: Caruso (1999)

4.2 *Risco*

Uma das definições de risco é que ele poder ser entendido como tudo aquilo que pode afetar os negócios e impedir que os objetivos sejam alcançados.

Um risco existe quando uma ameaça, com potencial para causar algum dano, apresenta alto índice de probabilidade de ocorrência no ambiente computacional e um baixo nível de proteção.

Como todos os ativos da empresa estão sujeitos a vulnerabilidades em maior ou menor escala, podendo significar riscos para a empresa, resultam muitas vezes de falhas nos seus controles. Logo, pode-se dizer que os riscos surgem em decorrência da presença de fraquezas e, por conseguinte, vulnerabilidades.

Por outro lado, as ameaças exploram as vulnerabilidades existentes que decorrem de falhas de configuração ou inexistência de medidas de proteção adequadas. Neste caso, os danos causados pela ação das mesmas causam impactos negativos no negócio, aumentando ainda mais os riscos.

O Gerenciamento de Riscos é um processo contínuo, que não termina com a implementação de uma medida de segurança. Através de monitoração constante, é possível identificar quais áreas foram bem sucedidas e quais precisam de revisões e ajustes (GERENCIAMENTO...2001).

5 **VULNERABILIDADE**

No ambiente da segurança podem-se considerar vulnerabilidades como falhas ou fraquezas que, se exploradas, ensejam na perda ou no vazamento de alguma informação. As vulnerabilidades podem ser encontradas no modo de agir das pessoas (por exemplo, aquelas que emprestam suas senhas a outros usuários), nos equipamentos (facilidade de se abrir um servidor, para ali colocar um equipamento de acompanhamento de teclado, ou falhas nos equipamentos de rede que podem ser exploradas por um *DOS*, por exemplo), ou nos sistemas ou softwares (erros que permitem a execução remota de aplicativos com privilégios de administrador num *web server* ou presença de software malicioso, por exemplo). Pelas razões abordadas é fundamental identificar as vulnerabilidades que podem contribuir para a ocorrência de incidentes de segurança, que é um aspecto importante na identificação de medidas preventivas.

Os riscos não podem ser determinados sem o conhecimento de até que ponto onde um sistema é vulnerável, à ação das ameaças. Em um processo de análise de segurança, devem-se identificar os processos críticos vulneráveis e saber se os riscos a ele associados são aceitáveis ou não. O nível de vulnerabilidade decai à medida em que são emplementados controles e medidas de proteção adequadas, diminuindo também os riscos para o negócio. Pode-se dizer que os riscos estão ligados ao nível de vulnerabilidade que o ambiente possui, pois para se determinar os riscos, as vulnerabilidades precisam ser identificadas (MOREIRA, 2001, p. 22-23)

5.1 *Tipos de vulnerabilidades*

Segundo Moreira (2001, p. 27), mencionam-se outras vulnerabilidades, também presentes em muitos ambientes, e que muitas empresas não atentam para determinadas situações:

a) senhas fracas;
b) falhas de implementação de segurança;
c) deficiência na Política de Segurança;
d) manuseio inadequado de informações confidenciais/críticas.

As principais vulnerabilidades encontradas costumam ser relativas a erros, acidentes ou desconhecimento dos usuários que, impensadamente alteram configurações de equipamentos, divulgam contas e senhas de acesso, deixam sessões abertas na sua ausência, utilizam senhas frágeis facilmente descobertas (como o próprio nome ou palavras comuns) ou mesmo contaminam seus arquivos e programas com vírus de computadores (BASTOS, 1998).

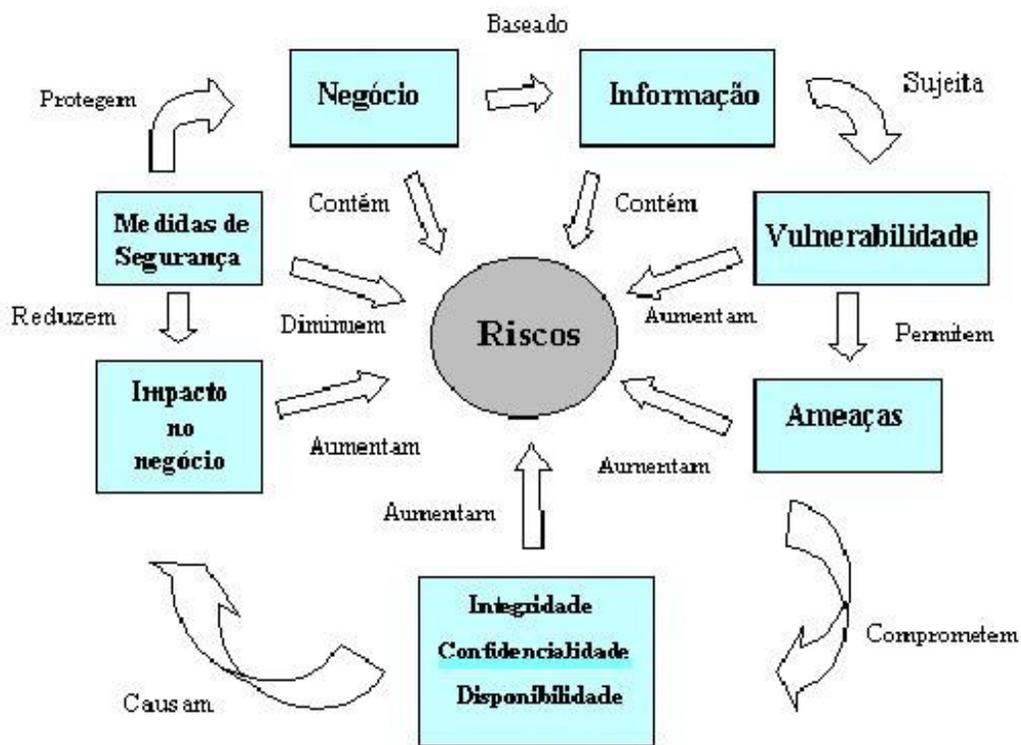



Figura 2 - Ciclo da Segurança da Segurança da Informação
Fonte: Moreira (2001)

6 **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

6.1 *Objetivos*

Apesar de a maioria dos executivos das Empresas estarem conscientes da necessidade da criação e cumprimento de uma Política de Segurança da Informação, faz-se necessário um esforço grande para que as Unidades de Segurança possam lançar mão dos recursos necessários para esta criação e manutenção. Portanto, cumpre identificar as soluções existentes voltadas a esta necessidade.

6.2 *Controles necessários*

Uma Política de Segurança da Informação (POLÍTICA...,2000), deve prover controles nos ambientes corporativos, quais sejam:

a) *software* de detecção de vírus e "cavalos de tróia";
b) *software* de controle de acesso lógico;
c) mecanismos de controle de acesso físico.

A Política de Segurança da Informação, deve envolver os seguintes agentes (POLÍTICA, 2000)

a) Gestor da Informação - o indivíduo responsável para fazer decisões em nome da organização no que diz respeito ao uso, à identificação, à classificação, e à proteção de um recurso específico da informação.

b) Custodiante - agente responsável pelo processamento, organização e guarda da informação.

c) Usuário - alguma pessoa que interage diretamente com o sistema computadorizado. Um usuário autorizado com poderes de adicionar ou atualizar a informação. Em alguns ambientes, o usuário pode ser o proprietário da informação.

6.3 *Classificação de informações*

De acordo com (POLÍTICA...2000), todo tipo de documento de uma corporação, deve exibir de maneira clara, o respectivo grau de acessibilidade ou seja

seu grau de sigilo, o que requer classificar todas as informações segundo o seu grau de criticidade e âmbito de acesso:

a) informações Confidenciais: só podem ser disseminadas para empregados previamente nomeados;
b) informações Corporativas: sua divulgação restringe-se ao âmbito da Empresa.
c) informações Públicas: podem ser disseminadas dentro e fora da Empresa.

A política de segurança precisa contemplar as seguintes facetas (POLÍTICA...2000):

Política de acessos externos à Instituição

a) definição de Convênios para acesso às bases corporativas;
b) criptografia;
c) certificação;
d) *log* de acessos;
e) configuração de *Firewall.*

Política de uso da Intranet

a) padrão de *Home-Page*;
b) padrão de Gerenciamento de Rede;
c) padrão de distribuição de versões de *software*;
d) modelo de identificação de pirataria;
e) detecção e inatividade de *Modens* ligados a rede;
f) padrão de atualização de anti-vírus.

Política de uso da Internet

a) acesso de Empregados ao Provedor Corporativo;
b) padronização da *Home-Page* Institucional;
c) padronização da *Home-Page* Comercial;
d) criptografia;
e) certificação;
f) configuração do *Firewall*;

g) roteamento;
h) eventos mínimos a serem logados nos Sistemas Corporativos;
i) trilhas de auditoria;
j) política de *Backup*.

<u>Política de uso de *software*</u>

a) dontrole antipiratária;
b) definição da linha-mestra dos *softwares* utilizados por ambiente computacional.

<u>Política de Acesso físico</u>

a) controle de acesso físico;
b) definição de ambientes físicos de alta criticidade;
c) monitoração de ambientes.

<u>Política de Acesso Lógico</u>

a) política de senhas e de identificação de usuário;
b) definição de perfis de acesso aos ambientes e aplicativos;
c) *Log* de Eventos Mínimos nas transações:
    * Dia e hora do acesso;
    * Endereço eletrônico de quem acessou;
    * Ações executadas.

Uma política de segurança também significa delegar responsabilidades para funcionários, que passam a responder por seus atos (se colaboram para a disseminação de um vírus, por exemplo). A importância da conscientização da equipe de profissionais é consenso entre os especialistas em segurança (BARBOSA, 2001, p. 27).

7 **CONTROLE DE ACESSO FÍSICO**

7.1 *Segurança Física*

A segurança física pode ser abordada de duas formas: segurança de acesso, que trata das medidas de proteção contra acesso físico não-autorizado; e segurança ambiental, que trata da prevenção de danos por causas naturais.

Os controles de acesso físico têm como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo o acesso a esses recursos. Apenas as pessoas expressamente autorizadas pela gerência podem ter acesso físico aos sistemas de computadores.

7.2 *Recursos a serem protegidos*

Os recursos a serem protegidos pelos controles de acesso físico são os equipamentos, a documentação e suprimentos. A proteção física desses recursos constitui-se em uma barreira adicional e anterior às medidas de segurança de acesso lógico. Pode-se dizer que os controles de acesso físico protegem os recursos lógicos.

8 **CONTROLE DE ACESSO LÓGICO**

Dentre os controles de acesso lógico, podemos destacar:

8.1 *Segurança lógica*

É a capacidade de garantir que um usuário é de fato quem ele diz ser. É uma das funções de segurança mais importantes que um sistema operacional deve fornecer (CONCEITOS – SEGURANÇA...,2001).

8.2 *Senha*

Senha de acesso é o método mais utilizado, pelas empresas para a autenticação de usuários. Para garantir o seu uso adequado, deve ser definida uma política de senhas, em que sejam criadas regras para a criação, troca e uso das mesmas. As regras definidas devem ser divulgadas entre todos os funcionários e colaboradores da organização. Um usuário, com uma senha fraca, pode ser

considerado uma grande vulnerabilidade, colocando em risco a segurança de todos os sistemas, tornando-os fáceis de quebrar ou descobrir (CONCEITOS – SEGURANÇA ..., 2000).

9 **PRINCIPAIS AMEAÇAS DE SEGURANÇA**

Em políticas de segurança citam-se as principais ameaças que devem ser consideradas pela política de segurança da Informação:

9.1 *Integridade*

a) ameaças de ambiente (fogo, enchente, tempestade ...);
b) erros humanos;
c) fraudes;
d) erro de processamento.

9.2 *Indisponibilidade*

Falhas em sistemas ou nos diversos ambientes computacionais

9.3 *Divulgação da informação*

a) divulgação de informações premeditada;
b) divulgação de informações acidental.

9.4 *Alterações não-autorizadas*

a) alteração premeditada;
b) alteração acidental.

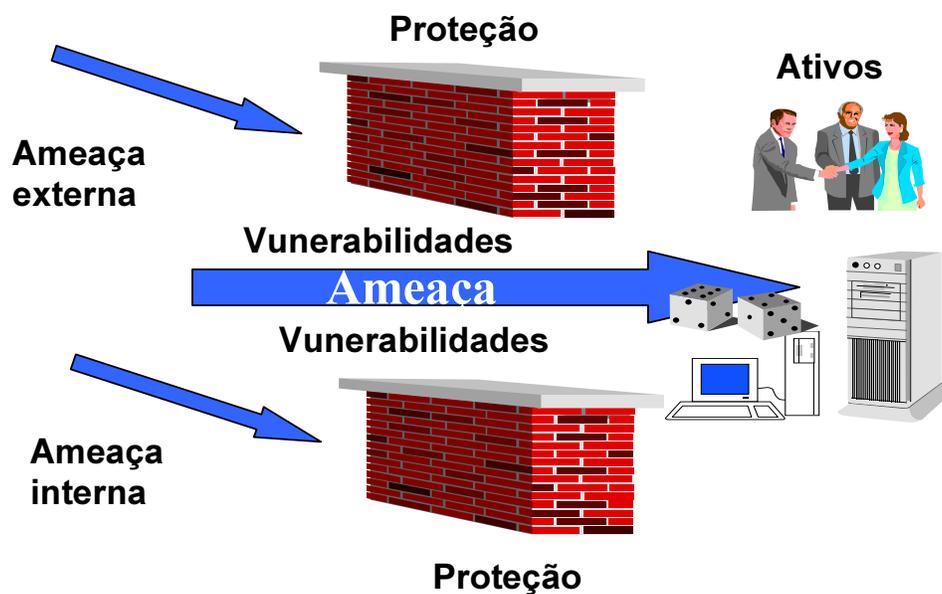



Figura 3 - Ameaças da segurança
Fonte: Moreira (2001)

10 **ORIGENS DAS AMEAÇAS**

É consenso na área de segurança que as ameaças podem ter duas origens: interna e externa.

10.1 *Ameaças internas*

Estão presentes no dia-a-dia das organizações independente de estarem conectados ou não a Internet. Sua existência é prejudicial para os negócios da empresa, cada qual com seu grau de periculosidade, podendo ser desde um procedimento inadequado de um funcionário, até uma ação internacional, com o intuito de interromper a execução de um processamento em determinado sistema (MOREIRA, 2001, p. 47).

Segundo (MOREIRA, 2001, p. 48), alguns exemplos de ameaças internas:

a) contaminação por vírus de computador através de um simples disquete;
b) incêndios;
c) funcionários mal treinados;
d) divulgação das senhas dos funcionários;
e) lixo informático;
f) falta de definição clara de responsabilidades;
g) falta de Procedimentos de Contingência;
h) uso indevido dos serviços de Internet em nome da empresa;
i) funcionários de empresas terceirizadas não familiarizado com a Política de Segurança da empresa.

10.2 *Fraudes cometidas por funcionários*

A fraude pode ser entendida, segundo Moreira (2001, p. 48), como qualquer tipo de exploração em um sistema com o objetivo de enganar a empresa através de alguma forma ou recurso. Apesar de ser possível na maioria dos casos detectar as fraudes, o sistema computacional da empresa precisa estar precavido a ponto de poder rastrear todas as operações efetuadas pelo fraudador.

Entre as fraudes podemos citar:

a) roubo de senhas;

b) uso indevido de conta e senha com grande nível de acesso na rede interna da empresa;
c) decodificação seguida de alteração de programas executáveis;
d) acesso à alteração de dados direto em banco de dados.

As empresas treinam seus empregados para conseguirem melhores resultados, mas se esquecem de treina-los para resguardar o seu mais valioso produto: a informação (PESQUISA...2002).

Ameaça	%
1º Funcionário insatisfeito	53%
2º Acessos indevidos	45%
3º Vírus	42%
4º Divulgação indevida	39%
5º Hackers	36%
6º Uso de notebooks	33%
7º Vazamento de informações	30%
8º Divulgação de senhas	30%
9º Fraudes, erros e acidentes	29%
10º Pirataria	27%
11º Falhas na segurança física	27%
12º Roubo de senhas	25%
13º Roubo / furto	24%
14º Super poderes de acesso	23%
15º Alteração indevida	21%
16º Uso indevido de recursos	21%
17º Alteração indevida de configurações	21%
18º Fraudes em e-mail	19%
19º Lixo informático	19%
20º Acessos remotos indevidos	19%
21º Concorrentes	18%
22º Espionagem industrial	18%
23º Incêndio / desastre	16%
24º Falhas de energia	15%
25º Sabotagens	12%

Gráfico 1 - Principais ameaças às informações da empresa:
Fonte: Pesquisa Nacional (2001)

10.3 *Roubo de informações*

O roubo de informações, conforme Moreira (2001, p. 49), ocorre não somente quando os computadores e *notebook* são roubados fisicamente, mas também quando são subtraídas as informações que eles contêm. Pode acontecer todos os dias, sendo necessário por parte da empresa trabalhar a conscientização dos funcionários com o intuito de evitar a conivência com ações como esta. Os meios podem ser:

a) *e-mail*;

b) relatórios;
c) cópia de dados em algum tipo de dispositivo de armazenamento (disquete, *Cd-Rom*, etc.).

10.4 *Erros humanos*

O fator humano, segundo muitas pesquisas, tem se mostrado uma das fontes mais comuns de incidentes de segurança, sendo que, em geral, a falta de treinamento e de suporte, omissões por parte dos funcionários acabam por se tornar a principal causa. O fator humano é objeto de constante preocupação por parte dos profissionais que projetam sistemas de segurança. Muitas vezes funcionários com acesso autorizado, porém desatentos e com pouco treinamento, podem tornar-se causa potencial de incidentes segurança (MOREIRA, 2001, p. 49).

10.5 *E-mail*

Conforme Moreira (2001, p. 50), existem vários riscos quando o assunto é *e-mail*. Desde falsificação até contaminação por vírus. Apesar de ser um meio eficiente de se trocar informações, ultimamente têm surgido diversas formas de burlá-lo e torná-lo um meio de propagar vírus pela Internet. O *e-mail* em uma organização deve ser utilizado para propósitos comerciais, mas comumentemente é utilizado para propósitos particulares, para fazerem *spam*, e outros fins que não o de negócios. Um outro aspecto que deve ser avaliado é o uso de Certificação Digital nos *e-mails* da empresa. Dessa forma, evita-se o não repúdio, garantindo a integridade não só da mensagem, mas dos arquivos anexos. Existem empresas que monitoram o conteúdo dos *e-mails* enviados pelos seus funcionários para fins de auditoria e/ou investigação.

As empresas treinam seus empregados para conseguirem melhores vendas e resultados, mas esquecem de treiná-los para resguardar o seu mais valioso produto: a informação (PESQUISA....,2002).

10.6 *Vírus*

Um vírus de computador é um programa pequeno desenvolvido para alterar a forma como um computador opera, sem a permissão ou o conhecimento do seu

usuário. Um vírus precisa atender a dois critérios. Primeiro, ele deverá executar a si próprio, freqüentemente inserindo alguma versão do seu próprio código no caminho de execução de outro programa. Segundo, ele deve se disseminar. Por exemplo, ele pode se copiar em outros arquivos executáveis ou em discos que o usuário acessa. Os vírus podem invadir tanto computadores como servidores de rede (CENTRO DE EDUCAÇÃO ANTIVÍRUS, 2002).

Algumas formas mais comuns para se infectar um sistema com vírus, nos dias de hoje (MOREIRA, 2001, p. 51):

a) anexos de mensagens recebidas via e-mail;
b) arquivos infectados armazenados em Servidores FTP;
c) arquivos recebidos via ICQ;
d) disquetes;
e) BBS;
f) *newsgroups*.

10.7 *Treinamento inadequado*

O treinamento é um fator importante em qualquer atividade, assim como a Segurança da Informação, pois envolve o comprometimento e a mudança no comportamento em muitas situações por parte dos funcionários. O comprometimento está relacionado com a participação e conscientização de todos os colaboradores da empresa, na implantação e continuidade das normas de segurança da corporação . Dessa forma, estagiários, temporários, terceiros, ou seja, do *Office-boy* ao presidente, todos devem estar comprometidos e participando deste processo.

10.8 *Pirataria*

Existem alguns tipos de pirataria, que se podem considerar como uma ameaça interna, dentre elas (MOREIRA, 2001, p. 54-55) cita:

Pirataria de *Software* - a pirataria de *software* é uma prática ilícita, caracterizada pela reprodução e/ou uso indevido de programas de computadores (*software*) legalmente protegidos, sem a autorização expressa do titular da obra e, conseqüentemente, sem a devida licença de uso.

Sabe-se que cada pacote de *software* vendido com uma única licença de usuário só pode ser usado em uma máquina; copiá-lo para outra máquina, mesmo que para o mesmo usuário, constitui pirataria. Alguns *softwares*, entretanto, possuem cláusulas no seu contrato de licença que permitem que cópias sejam feitas, desde que seguidas algumas normas, como por exemplo, a sua utilização por um número limitado de usuários (como geralmente acontece com programas para redes locais).

Desta forma, ao adquirir um programa de computador, o usuário não se torna proprietário da obra. Ele está apenas recebendo uma licença de uso, que é uma permissão para o uso, de forma não exclusiva. Mesmo tendo adquirido uma cópia original, o usuário não possui o direito de comercializar, a não ser que tenha autorização expressa do titular da obra.

Em certos casos, ao comprar um *software*, o usuário pode fazer uma cópia de "backup", para fins de segurança e para seu próprio uso. Esta cópia só poderá ser efetuada com uma permissão específica do detentor dos direitos autorais.

Pirataria Coorporativa - ocorre quando há execução de cópias não-autorizadas de *software* em computadores dentro de organizações. Esta é uma das formas de pirataria mais difundidas, sendo responsável por mais da metade das perdas sofridas. Ela acontece quando são feitas cópias adicionadas de *software* pelos empregados, para uso sem a aquisição de novas licenças o que, mesmo em pequenas quantidades, pode significar multas vultuosas, desgaste da imagem da empresa, entre outros.

Pirataria Individual – representa o compartilhamento de softwares com amigos e/ou colegas de trabalho.

Também é um problema significativo, especialmente porque os usuários individuais, que fazem cópias não-autorizadas, não acreditam que possam ser detectados, pois o número de pessoas que praticam esta contravenção é muito grande. Porém, a lei vale para todas as modalidades de transgressão, inclusive para a pirataria individual.

10.9 *Ameaças externas*

Representam todos os ataques oriundos de fora do ambiente da Organização com o objetivo de explorar as vulnerabilidades de um determinado sistema computacional para uma finalidade qualquer. Elas representam um alto grau de participação nas pesquisas sobre ataques a sistemas computacionais. Com a prática do comércio eletrônico, estes números vem aumentando a cada dia, assim como as formas de ataques (MOREIRA, 2001, p. 60).

10.9.1 Invasores

São pessoas que se aventuram a utilizar seus conhecimentos com ferramentas e técnicas para burlarem esquemas de segurança computacional.

Alguns tipos comuns de invasores, citados por, Moreira (2001, p. 64-67):

Hacker – é um indivíduo que sempre quer saber mais, investiga extensivamente os sistemas para detectar más configurações, “bugs” e buracos nas configurações que permitem ganhar acesso aos sistemas. Ao contrário do *cracker*, o *hacker*, depois de entrar no sistema, não altera a informação, pois esta atitude vai contra a ética dos *hackers*. Só entram no sistema para o explorar e para se divertir, utilizar recursos (grandes computadores com enorme capacidade de processamento), ou como ponto de passagem.

Cracker – é definido por alguns como um *hacker* mal intencionado, porque invade computadores e *homepages*, não por divertimento, mas por interesses próprios para desviar a conexão para outra página (concorrente, por exemplo), tirar algum serviço do ar.

Phreaker – tem bons conhecimentos de telefonia e consegue inclusive fazer chamadas internacionais sem pagar, o que lhe permite desenvolver seus ataques a partir de um servidor de outro país. Enquanto as companhias telefônicas aprimoram suas defesas, os *pheakers* buscam novas possibilidades de fraudá-las.

Lammer – Indivíduo que se utiliza de programas para invadir *sites*.

Outro ponto a ser destacado são os motivos pelas quais pessoas mal intencionadas praticam atos de cunho maldosos. Eis alguns dos motivos dessas causas (MOREIRA, 2001, p. 61-64):

Ganhos Financeiros – alguns funcionários com certo conhecimento do processo, ou com um certo grau de poder, obtêm acesso a sistemas financeiros da empresa para desviar dinheiro (através de transferência eletrônica, por exemplo). Geralmente, esses funcionários ganham menos do que outros que possuem o mesmo tempo de empresa.

Vingança – importante motivação para entradas não-autorizadas em sistemas e redes é a vingança de funcionários. O risco de atividades não-autorizadas envolvendo o uso de computadores, aumenta substancialmente quando surgem funcionários dispensados, demitidos, rebaixados, preteridos em promoções, mal pagos ou tratados de forma injusta. O não-cancelamento do acesso remoto a sistemas e a outros recursos computacionais acaba criando um canal conveniente para os motivados por vingança. Os estudos de caso sugerem que a vingança é a causa mais provável de ocasionar problemas ou danos a sistemas do que a maioria dos outros motivos.

Anarquia – os anarquistas penetram nos sistemas simplesmente para produzir a discórdia e a segregação. Esses intrusos são motivados pela emoção provocada pelo desenvolvimento de atividades não-autorizadas.

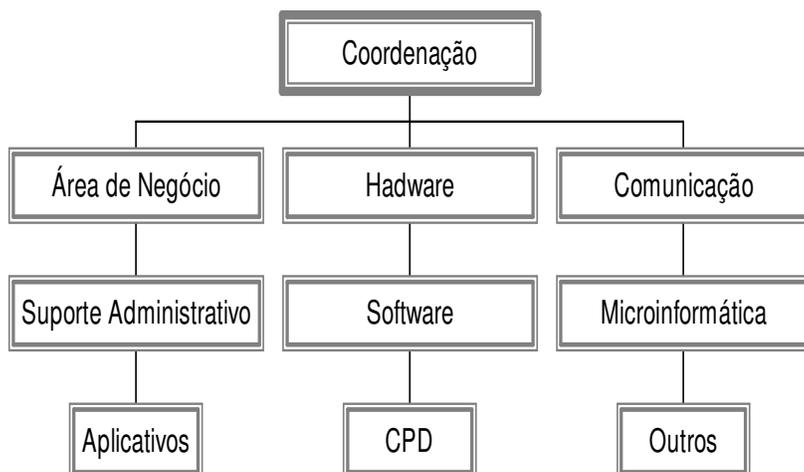
Idealismo – alguns intrusos atacam sistemas por razões idealistas. Eles se vêem como heróis protegendo o mundo de operações clandestinas de coleta de dados por parte do governo.
Outros afirmam que estão encontrando pontos vulneráveis para tornar as redes e os sistemas mais seguros.
Outros vêem a informática como uma atividade aberta que não deveria ser restrita por medidas de controle de segurança.

Espionagem Industrial – ocorre quando pessoas ou organizações se dedicam a atividades ilegais contra outra empresa. Vários casos de crimes envolvendo o mau uso do computador mostram que um ou mais funcionários de uma empresa tentaram

violar os recursos de informática de outra empresa para obter uma vantagem competitiva ou para roubar *software* a serem comercializados, projetos, etc.

11 **PLANO DE CONTIGÊNCIA**

Consiste em procedimentos de recuperação preestabelecidos, com a finalidade de minimizar o impacto sobre as atividades da organização no caso de ocorrência de um dano ou desastre que os procedimentos de segurança não conseguiram evitar (CARUSO, 1999, p. 289).

O objetivo de um plano de contingência é servir como guia para esquematizar a execução de ações a serem tomadas para a continuidade dos serviços essenciais das áreas de negócios que dependam de um computador. Num plano de contingência não é preciso necessariamente utilizar equipamentos similares aos envolvidos no evento gerador da contingência (CARUSO, 1999, p. 291).

Fluxograma 1: Modelo de esquema organizacional para grupos de contingência.
Fonte: Caruso (1999)

Para mostrar-se eficaz, o Plano de Contingência deve receber o apoio da direção da empresa ou instituição, definindo-se assim responsabilidades, formando-se grupos voltados no desenvolvimento, treinamento, manutenção e execução da segurança de informações.

Havendo um plano de contingência, o risco será plenamente conhecido e identificado, evitando assim, problemas de *software* ou de *hardware*, falhas nas comunicações e no fornecimento de energia e de pessoal, entre outros.

12 **AUDITORIA**

Consiste em um serviço de apoio da Empresa, cuja natureza é a de um controle que implica examinar e avaliar a adequação e eficiência de outros controles.

O objetivo da auditoria consiste em apoiar os membros da empresa no desempenho de suas atividades. Para tanto a auditoria lhes proporciona análises, avaliações, recomendações, assessoria e informação concernente às atividades revisadas (AUDITORIA....,2001).

12.1 *Auditoria interna*

A auditoria interna é responsável pela revisão independente dos processos de gestão ou direção, compreendendo o seu alcance a todas as partes que integram a empresa vale dizer, inclui as atividades técnicas, comerciais, financeiras, contábeis e de sistemas de informação e gestão. Sua missão é de subministrar um serviço de valoração construtiva da totalidade das atividades da empresa. Para isso escolhe as operações e atividades que serão submetidas à auditoria e que poderão beneficiar-se com a revisão que esta fizer, (AUDITORIA...,2001).

O objetivo da auditoria é avaliar se a Empresa está operando dentro dos padrões desejados pela política de segurança da informação. A auditoria responde pela Direção da Empresa nas diversas áreas estratégicas.

13 **CONCLUSÃO**

Na elaboração desse trabalho constatou-se que a Segurança de Informações é o elemento chave dentro da organização: envolve aspectos técnicos, humanos e organizacionais, sendo fundamental a definição e existência de uma Política para efetiva proteção das informações. O objetivo da segurança da informação é proteger a empresa contra riscos, apoiada em um Plano de Cultura de Segurança e uma estrutura de Planejamento de Segurança, onde se podem identificar as vulnerabilidades e ações pró-ativas para a proteção das informações.

A pesquisa evidenciou que, na era do conhecimento, a informação é considerada um dos principais patrimônios de grande parte das organizações, devendo ser tratada como tal, e protegida nos seus aspectos de disponibilidade, integridade, confidencialidade e autenticidade. Segurança é responsabilidade e dever de todos e, como tal, deve ser de conhecimento de cada profissional da empresa o cumprimento e conscientização de medidas de proteção dos recursos da informação, pois se trata de questão de alta prioridade.

Percebe-se que a tarefa de implementação das principais práticas de segurança da informação na corporação não é uma tarefa fácil, mesmo quando se trata de uma empresa de pequeno porte. Envolve fatores objetivos e subjetivos que, ao se somarem, representam um caso diferenciado, impossível de ser traduzida em uma fórmula. Todavia, o ato de uma conscientização ampla da necessidade da adoção das práticas de segurança já é um grande passo tomado pela organização. Sempre lembrando que o melhor caminho não é a implantação compulsória, e sim a disseminação da cultura entre cada um dos ambientes da empresa. Afinal, nem todos os colaboradores e funcionários entendem a necessidade de mecanismos de controle e de gerenciamento da segurança da informação.

Esse foi o objetivo principal deste trabalho: demonstrar que a Segurança da informação deve ser a mobilização de interesses comuns, coletivos e difusos em prol da defesa e fortalecimento do patrimônio intangível – a informação -, um dos bens mais valiosos de qualquer organização.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023:** Informação e documentação: referências: elaboração. Rio de Janeiro, 2002.

_________. **NBR 6024**: numeração progressiva das seções de um documento. Rio de Janeiro, 1989.

_________. **NBR 6027**: sumário. Rio de Janeiro, 1989.

_________. **NBR 6028**: resumos. Rio de Janeiro, 1990.

_________. **NBR 6033**: ordem alfabética. Rio de Janeiro, 1989.

_________. **NBR 10520**: informação e documentação: citações em documentos: apresentação. Rio de Janeiro, 2002.

_________. **NBR 14724**: informação e documentação: trabalhos acadêmicos: apresentação. Rio de Janeiro, 2002.

AUDITORIA – ANACAP. 2001. Disponível em: <http//www.ancap.com.uy/portugueses/auditor1.htm>. Acesso em: 1 ago. 2002.

AXUR IINFORMATION SECURITY – especializada em seguranaça da informação. [200-?]. Disponível em: <http://www.axur.com.br/gestao.htm>. Acesso em: 12 jun. 2002.

BARBOSA, Alexandre. E-business com segurança. **Internet Business,** São Paulo, ano 5, n. 49, p. 27, set. 2001.

BASTOS, Alberto. **Gerenciando a Segurança das Informações nas Empresas**. 1998. Disponível em: <http://modulo.com.br/empresa/...as/artigo_entrevista/a-gerenc.htm>. Acesso em: 5 abr. 2002.

CAMARÃO, Paulo Cesar Bhering. **Glossário de informatica**. Rio de Janeiro: LTC, 1994.

CARUSO, Carlos A. A. **Segurança em informática e de informações**. São Paulo: SENAC, 1999.

CENTRO DE EDUCAÇÃO ANTIVÍRUS. 2002. Disponível em: <http://www.symantec.com/region/br/avcenter/education>. Acesso em: 8 ago. 2002.

COLTRO, Renata. Segurança: prioridade coorporativa. **Computerworld,** São Paulo, p. 26, 13 mar 2002.

CONCEITOS – segurança lógica – autenticação. 2000. Disponível em: <http://www.scua.net/seguranca/conceitos/seglogica_autenticacao.htm>. Acesso em: 12 dez. 2001.

CONCEITOS de segurança – TI. 2000. Disponível em: <http://www.ti.petrobras.com.br/gcom/seguranca/>. Acesso em: 25 jul. 2002.

FRAGOMENI, Ana Helena. **Dicionário enciclopédico de informática**. Rio de Janeiro: Campus, 1986.

FREEDMAN, A. **Dicionário de Informática**. São Paulo: Makron Books, 1995.

GERENCIAMENTO de riscos. 2001. Disponível em: <http://www.securenet.com.br/>. Acesso em: 30 jun. 2002.

INTERSIX Technologies. 2002. Disponível em: <http://www.intersix.com.br>. Acesso em: 12 jul. 2002.

MÓDULO Security Solutions S/A. 2002. Disponível em: <http://www.modulo.com.br>. Acesso em: 20 jun. 2002.

MOREIRA, Stringasci Nilton. **Segurança mínima**: uma visão coorporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

NETSECURITY Systems. 2002. Disponível em: <http://www.netsecurity.com.br>. Acesso em 05 ago. 2002.

PESQUISA nacional sobre segurança da informação. 2001. Disponível em: <http://www.modulo.com.br>. Acesso em: 22 ago. 2001.

PESQUISA revela falta de padrões de segurança em grandes empresas. 2002. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em: 9 abr. 2002.

PFAFFENBERGER, Bryan. **QUE**: dicionário dos usuários de microcomputadores. Rio de Janeiro: Campus, 1992.

POLÍTICA de segurança da informação. 2000. Disponível em: <http://geocities.yahoo.com.br/jasonbs_1917/seguranca/politica.htm>. Acesso em: 29 maio. 2002.

POLÍTICAS e diretrizes. 2002. Disponível em: < http://www.serinf.petrobras.com.br/politicas/politica.htm>. Acesso em: 21 maio. 2002.

PROTEUS Security Systems. 2002. Disponível em: <http://www.proteus.com.br>. Acesso em 05 ago. 2002.

SCUA Information Security Ltda. 2002. Disponível em: <http://www.scua.net>. Acesso em: 10 jul. 2002.

SECURENET. 2002. Disponível em: <http://www.securenet.com.br>. Acesso em 10 jul. 2002.

SEGURANÇA da tecnologia. 2001. Disponível em: <http://www.modulo.com.br>. Acesso em: 07 fev. 2002.

SEGURANÇA e competência. 2001. Disponível em: <http://www.procwork.com.br/Outsourcing/outsuporte_tecn.htm>. Acesso em: 30 jul. 2002.

STAR point - glossário de termos de informática. [200-?]. Disponível em: <http://www.startpoint.com.br/glossar.htm>. Acesso em: 25 jul. 2002.

SYMANTEC do Brasil. 2002. Disponível em: <http://www.symantec.com.br>. Acesso em: 12 jul. 2002.

TI BRASIL Intelligence. 2002. Disponível em: <http://www.ti-inteligence.com.br>. Acesso em: 03 ago. 2002.

WEBOPEDIA. 2002. Disponível em:<http://webopedia.com>. Acesso em: 30 jul. 2002.

GLOSSÁRIO

Bbs – serviço eletrônico que oferece recursos como correio eletrônico, acesso a outros computadores e serviços remotos, meios de oferecer e receber arquivos de domínio público, conversas *on-line*. O acesso ao BBS pode ser feito via modem, por discagem direta, de forma independente, sem o uso de uma rede (PFAFFENBERGER, 1992, p. 49).

Bugs – defeito, erro de *hardware* ou *software* (FRAGOMENI, 1986, p. 60).

Criptografia – processo de codificação dos dados de modo a impedir sua leitura por usuários que não disponham da senha correta (PFAFFENBERGER, 1992, p. 118).

Firewall – combinação de *hardware* e *software* cujo papel é o de filtrar o trânsito de informações entre redes fechadas (como as de uma empresa) e a Internet. Impede que usuários não autorizados entrem nesta rede interna, via Internet, ou que dados de um sistema caiam na Internet, sem prévia autorização. Usa sistemas de monitoração que olham tudo o que entra e sai do servidor e outros protocolos de segurança (PFAFFENBERGER, 1992, p. 182).

FTP – protocolo de Transferência de Arquivos. Ferramenta que permite transferir arquivos e programas de uma máquina remota para a sua, e vice-versa na Internet. Também é utilizado para designar o programa que realiza a transferência dos arquivos (CAMARÃO, 1992, p. 222).

Home Page - página inicial de qualquer endereço eletrônico com conexão, para outros servidores da Internet ou ainda para entradas de hipertexto (WEBOPEDIA, 2002).

HTTP - um protocolo cliente/servidor usado para compartilhar informações na Internet. Ele é a base da *Worldwide Web* (WWW) (FREEDMAN, 1995, p. 241).

Icq – software usado para que pessoas possam se achar, trocar mensagens, permite saber quem está conectado, enviar arquivos e mensagens (ainda que não conectado), jogos em parceria on-line e seções de bate-papo (FREEDMAN, 1995, P. 245).

Logs – registros de uma operação com arquivo(s). Arquivos *log* são relatórios de situações ou de rotinas específicas, úteis para recuperar informações sobre as condições do micro (CAMARÃO, 1992, p. 312).

Modem – dispositivo eletrônico que converte os sinais enviados pelo computador em sinais de áudio, que serão enviados ao longo das linhas telefônicas e recebidos por outro *modem* que irá receber o sinal sonoro e convertê-lo de volta em sinais de computador. O modem também disca a linha, responde a uma chamada e controla a velocidade de transmissão (PFAFFENBERGER, 1992, p. 330).

News Groups – são grupos de discussões que usam *software* e servidores para trocarem informações (WEBOPEDIA, 2002).

Roteador – dispositivo de uma rede que recebe dados e os envia aos pontos de destino, sempre usando as rotas mais curtas disponíveis (PFAFFENBERGER, 1992, p. 443).

Spam – envio de mensagem por correio eletrônico sem que a mesma seja solicitada pelo seu destinatário (WEBOPEDIA, 2002).

Userid – identificador (*login*) associado a um arquivo ou nome de um usuário (podendo ser fictício) (CAMARÃO, 1992, p. 586).

Web – ver WWW.

Web Server – servidor WEB. Computadores dedicados a servir *home pages* para usuários na Internet, geralmente são estações. Um servidor ou computador hospedeiro, equipado para oferecer acesso *Web* aos clientes, que roda protocolo *http*, que pode ser acessado por clientes *Web* (WEBOPEDIA, 2002).

WWW – serviço Internet que liga documentos fornecendo conexões hipertexto entre servidores. Ele permite que o usuário pule de um documento para o documento relacionado, independente de onde ele esteja armazenado na Internet (FREEDMAN, 1995, p. 578).

ANEXO A - SITES DE EMPRESAS ESPECIALIZADAS EM SEGURANÇA DE INFORMAÇÕES

Figura 1
Fonte: MODULO Security Solutions S/A. 2002.

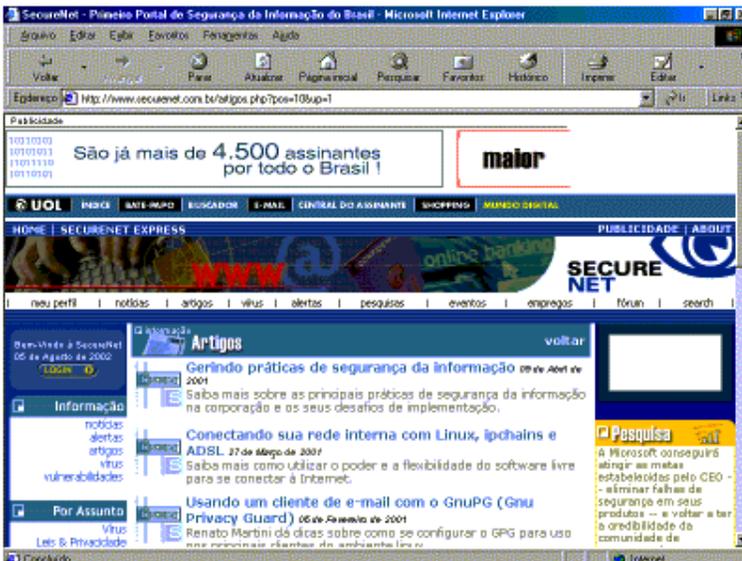



Figura 2
Fonte: SECURENET. 2002.

Figura 3
Fonte: SYMANTEC do Brasil. 2002.

Figura 4
Fonte: SCUA Information Security Ltda. 2002.

Figura 5
Fonte: IINTERSIX Technologies. 2002.

Figura 6
Fonte: NETSECURITY Systems. 2002.

Figura 7
Fonte: PROTEUS Security Systems. 2002.

Figura 8
Fonte: TI BRASIL Intelligence. 2002.